UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Entire digital contents of the Dropbox account(s) associated with the email account mikejacobsjr1989af@gmail.com and all its associated services, more fully described in Attachment A.

Case No. 24 MJ 54

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(5)(B) and (b)(2)	Possession of and access with intent to view child pornography

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Nathan A Cravatta

Applicant's signature

Nathan A. Cravatta, Special Agent HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means)*.

Date: 01/29/2024

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Nathan A. Cravatta, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been so employed since May 2005. I am currently assigned to the HSI Office of the Resident Agent in Charge in Milwaukee, Wisconsin. My duties include investigating criminal violations relating to child exploitation and child pornography including violations of advertising, producing, distributing, receiving, and possessing child pornography, in violation of Title 18, United States Code, Sections 2251 and 2252 and travel with the intent to engage in illicit sexual conduct, in violation of Title 18, United States Code, Section 2423(b). I have received training in the investigation of child pornography and child exploitation offenses and have observed and reviewed numerous examples of electronically stored child pornography.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc, an online electronic file storage provider headquartered at 1800 Owens Street, San Francisco, California 94158. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to

the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION AND APPLICABLE LAW

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

5. The following definitions applies to this Affidavit and Attachment B of this Affidavit:

a. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual

depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. "Cloud Storage" refers to saving data to an off-site storage system maintained by a third party. Instead of exclusively storing information to the computer's hard drive or other local storage devices, the user saves it to a remote database (and or both). The Internet provides the connection between the computer and the database. There are several cloud based storage options available to consumers (Dropbox, Google Drive, Box, Copy, Amazon, One Drive), with the majority of them offering gigabytes of storage free of charge.

d. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-

mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

e. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information, (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

f. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address, which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

g. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

h. The terms "records," "documents," and "materials," include all information recorded in any form, visual or aural, and by any means, whether in handmade form, (including, but not limited to, writings, drawings, painting), photographic form, (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form, (including, but not limited to, phonograph records, printing, typing), or electrical, electronic or magnetic form, (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

BACKGROUND ON NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

6. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

7. In addition to reports from the general public, reports are made by U.S. electronic communication service (ECS) providers and remote computing services (RCS), which are required by 18 U.S.C. § 2258A to report "apparent child pornography" to NCMEC via the CyberTipline if they become aware of the content on their servers. Specially trained analysts, who examine and evaluate the reported content, review leads, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

8. The CyberTipline receives reports, known as CyberTips, about the possession, production and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

9. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography.

DROPBOX

10. Based on my training and experience, and the training and experience of other law enforcement personnel with whom I have spoken, I have learned the following about Dropbox:

a. Dropbox is a privately held electronic file storage service provider headquartered in San Francisco, California. Dropbox utilizes cloud computing to enable users to store and share files and folders with other users across the Internet by way of file synchronization.[1] Once a file is added to a user's Dropbox account, that file

[1] File synchronization or "syncing" is the process of ensuring that computer files in two or more locations are updated by way of certain rules; file synchronization is commonly used for home backups on external hard drives or updating for transport on USB flash drives.

is synced to Dropbox's secure online servers. Dropbox provides both free and fee-based electronic file storage services.

b. Dropbox offers a client application to facilitate file synchronization and access on a wide variety of operating systems and devices owned or used by the account holder. Dropbox allows a user to create an account that is identified by the user's e-mail address and secured with a password. The e-mail address is the unique identifier for a Dropbox account.

c. Once an account is created with Dropbox, the default setting for the account is private, meaning that only the user can access the files and folders in the account. However, the user can share files or folders in the Dropbox account with others in a variety of ways. For example, a Dropbox user can share files or folders with other individuals who have Dropbox accounts; utilizing Dropbox's "Share a File" function, the user enters the name or e-mail address of the Dropbox account holder with whom the user wants to share a particular file or folder. A Dropbox user can also share files or folders with individuals who do not have Dropbox accounts; utilizing Dropbox's "Share a Link" function, the user creates a link to a file or folder that others can then use to view and download the material using their Internet browser.

WEB HOSTING COMPANIES

11. Based on my training and experience, and the training and experience of other law enforcement personnel with whom I have spoken, I have learned the following about web-hosting companies:

a. Web-hosting companies, such as Dropbox, maintain server computers connected to the Internet. Dropbox customers use those server computers to upload, download, store, access, and share electronic files.

b. In general, web-hosting companies like Dropbox ask each of their customers to provide certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, e-mail address, and telephone number. Web-hosting companies typically retain records concerning the length of service (including start date) and types of services utilized by their customers, as well as information concerning payments made by their customers for these services (including bank and credit card accounts used to make payments).

c. Web-hosting companies' customers typically place files, software code, databases, and other data onto the companies' servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several different ways. In some situations, it is possible for a customer to upload files using a special website interface offered by the web-hosting company. It is also possible for the customer to directly access the server computer through Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands and copy files to the web server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of connections, the method of connecting, and the IP addresses of the remote users' computers. Servers also commonly log the port number associated with the connection.

Port numbers assist computers in determining how to interpret incoming and outgoing data. SSH, Telnet, and FTP are generally assigned to different ports.

d. The servers use those files, software code, databases, and other data to respond to requests from Internet users for pages or other resources from the website. Commonly used terms to describe types of files sent by a server include HyperText Markup Language ("HTML") (a markup language for web content), Cascading Style Sheets ("CSS") (a language for styling web content), JavaScript (a programming language for code run on the client's browser), and image files. Web-hosting companies frequently allow their customers to store collections of data in databases. Software running on the web server maintains those databases; two common such programs are named MySQL and PostgreSQL (although these are not the only ones).

e. Web-hosting companies sometimes provide their customers with e-mail accounts. The contents of those e-mail accounts are also stored on the web hosting company's servers.

f. Websites deliver their content to users through the Hypertext Transfer Protocol ("HTTP"). Every request for a page, image file, or other resource is made through an HTTP request between the client and the server. The server sometimes keeps a log of all of these HTTP requests that shows the client's IP address, the file or resource requested, the date and time of the request, and other related information, such as the type of web browser the client uses.

g. In some cases, a subscriber or user will communicate directly with a web-hosting company about issues relating to a website or account, such as technical problems, billing inquiries, or complaints from other users. Web-hosting companies typically retain records about such communications, including records of contacts between the user and the company's support services, as well records of any actions taken by the company or user as a result of the communications.

12. Based on my training and experience in child pornography investigations, I know that a search of cloud storage account contents, like the **SUBJECT ACCOUNT**, often yields investigative leads relating to:

a. originals, computer files and copies of child pornography, as defined in 18 U.S.C. § 2256(8);

b. minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

c. communications with others, including minors, for the purpose of engaging in the possession, receipt, and/or distribution of child pornography;

d. the identities of co-conspirators and other individuals engaged in the possession, receipt, and/or distribution of child pornography;

e. the contact information of co-conspirators and other individuals engaged in the possession, receipt, and/or distribution of child pornography;

f. the timing of communications among co-conspirators and other individuals involved in the possession, receipt, and/or distribution of child pornography; and

g. the methods and techniques used in the possession, receipt, and/or distribution of child pornography.

PROBABLE CAUSE

Information Obtained from the West Allis Police Department

13. On March 10, 2023, West Allis Police Department Detective Jonathan Cerqua received and reviewed NCMEC CyberTip Report #153355224. According to information received from NCMEC, on January 19, 2023, at approximately 8:44 p.m. Central Standard Time (CST), Google became aware user "burning tempest," with an associated and verified email address of burningtempest1989@gmail.com and reported date of birth of April 5, 1989, uploaded one video labeled as "2 Boys molested.mp4". This file was stored in the Google Drive[2] infrastructure. Information provided by Google indicates portions of the file were reviewed by personnel to the extent necessary to confirm the file contained apparent child sexual abuse material.

14. On May 16, 2023, I reviewed the file associated with CyberTip Report #153355224 which is six minutes and fifty-three seconds in length. This file is described as follows:

> *This video begins with the camera being positioned in a small room. A twin bed with a red bedspread and large, white square designs is visible in the room. A wooden door is*

[2] Google Drive is a file storage and synchronization service which allows users to store files in the cloud, synchronize files across devices, and share files.

slightly opened and there are clothes handing in an armoire. A second bed is located near the aforementioned bed. A naked, white adult male is observed facing the camera. He is holding his erect penis in right hand and is actively masturbating. The wooden door opens and a naked, pre-pubescent male (MV-1), approximately seven to eight years old based on lack of pubic hair and body stature, enters the room, stands on the bed, and hold his penis with both hands. MV-1 is observed kneeling and looking directly at the camera. He can be heard speaking an unknown foreign language. A second naked, pubescent male victim (MV-2), approximately ten years old based on a noticeably larger body stature, who appears to be adjusting the camera, enters the view of the camera. He is observed holding his penis with his left hand and standing next to the adult male who continues to masturbate. The adult male places his left arm around the lower torso of MV-2 and pulls him closer. MV-1 steps closer to both of them while holding his penis in his right hand. He then stands on the bed and MV-1, MV-2, and the adult male touch the tips of their penises together. MV-1 gets off the bed and closes the door. MV-2 and the adult male are observed pressing their lower torsos and penises against each other. MV-1 is then visible pressing his naked torso against the lower back of the adult male. He then begins to make thrusting motions and the adult male places his left hand on MV-1's buttocks and pulls him closer to his body. All three individuals separate but continue to fondle their own erect penises. The adult male is then observed sitting on the bed and places MV-2's erect penis into his mouth and begins to perform oral sex. The adult male then uses his left hand to fondle MV-1's penis. The adult male stops performing oral sex on MV-2 and begin to perform oral sex on MV-1. The adult male then stops and resumes performing oral sex on MV-2. The adult male is then observed positioning himself on the bed on his hands and knees. MV-2 is observed placing his erect penis into the buttock area of the adult male and begins to make thrusting motions. MV-1 moves the camera closer to MV-2 and the adult male. MV-2 then grabs the camera from MV-1 and focuses on his erect penis being inserted into the buttock of the adult male. MV-1 then retrieves the camera and places it back to its original position. MV-1 then positions himself next to MV-2 and the adult male. MV-2 removes his penis from the buttocks area of the adult male. MV-1 briefly presses his penis against the adult male's buttocks. MV-1 is then observed laying on his back and the adult male straddles him while MV-2 positions himself behind the adult male. MV-2's body blocks the view of the camera. Laughing can be heard in the video. The adult male is then seen getting off of MV-1 who proceeds to get off of the bed. The adult male positions himself on his hands and knees on the bed. MV-1 positions himself near the buttock area of the adult male and engages in anal intercourse with the adult male for approximately thirty-one seconds. MV-1 steps away from the adult male. MV-2 is positioned near the bed and next to the adult male. The adult male begins to perform oral sex on MV-2 for approximately thirty-two seconds. MV-2 then positions himself near the buttock area of the adult male and inserts his erect penis in the adult male's anus and they begin to have anal intercourse. MV-1 briefly grabs the camera and moves it closer to show a close-up view of MV-2's penis inserted into the anus of the adult male. MV-1 and the adult male continue to have anal intercourse until the video concludes.

Based on my training and experience, the video as described above depicts child pornography

15. CyberTip Report #153355224 also provided IP login information associated with Google user "burning tempest". According to information received, on January 14, 2023, at 10:16 a.m., "burning tempest" accessed the account from IP address 2607:fb90:d38a:98c7:51f2:707d:b12f:4b09

16. On February 27, 2023, a State of Wisconsin-Office of the Attorney General administrative subpoena was issued to T-Mobile requesting subscriber records assigned to IP address 2607:fb90:d38a:98c7:51f2:707d:b12f:4b09 used on the previously noted date and time.

17. On March 6, 2023, T-Mobile produced the following subscriber records:

Subscriber Name: Michael Jacobs
Subscriber Address: 1711 South 68th St., West Allis, WI 53214
Begin Service Date: October 23, 2022
MSISDN No./Target Number: (920) 441-9678
IMSI: 310260549011182

18. On March 23, 2023, a search warrant was issued by the Milwaukee County Circuit Court to Google LLC for records and information associated with email address burningtempest1989@gmail.com.

19. On April 14, 2023, Google LLC produced the requested records to Detective Cerqua. Records provided indicate email address burningtempest1989@gmail.com was created on December 29, 2022. The name listed for this account is "burning tempest" with a date of birth of April 5, 1989. IP login

records were received from December 29, 2022 to January 14, 2022. This account was closed on January 19, 2023 at 6:02 p.m. CST.

20. A Google Pay[3] customer profile for this account lists the following information:

> Billing Name: Michael Jacobs
> Billing Address: 1711 S. 68th St., West Allis, WI 53214
> Instrument Description: PayPal: mikejacobs1989far@gmail.com
> Payment Profile Creation: December 29, 2022

21. Google internet search history records provided for this account indicates on January 5, 2023, the following search terms were entered, "family threesome MMF," "father son family threesome," "Incest tube," and "Family threesome mom son dad".

22. A review of email content indicates on January 12, 2023, at 3:34 a.m., burningtempest1989@gmail.com received an email from Ubisoft+<news@updates.ubisoft.com> with the subject line of "Confirmation of our subscription." This email lists subscription and billing information dated January 12, 2023. The billing address lists an address of 1711 S. 68th St., West Allis, WI 53214. Payment information lists a PayPal account of Mikejacobs1989ds@gmail.com.

23. On January 19, 2023, at 5:42 a.m., burningtempest1989@gmail.com sent an email to mikejacobs989fg@gmail.com with the subject line of "video". Attached to this email is a Google Drive link labeled, "2 boys molested.mp4."

---

[3] Google Pay is a mobile payment service developed by Google enabling in-app, online, and in-person contactless purchases on mobile devices, tablets, or watches.

24. On January 19, 2023, at 5:48 a.m., burningtempest1989@gmail.com sent an email to mikejacobs989fg@gmail.com with the subject line of "video". Attached to this email is a file labeled as, "video_2023-01-11_20-12-53.mp4". I have reviewed this file which is a video five minutes and twenty-five seconds in length and is described as follows:

> *The video begins with the camera focusing on a pubescent male minor (MV-3), approximately twelve years old based on body stature, performing oral sex on a pre-pubescent male (MV-4), approximately nine to ten years old based on body stature and lack of pubic hair, who appears to be laying down and wearing a turquoise-colored shirt. As the video begins an unknown individual can be heard stating, "You starting?" The MV-3 indicates, "Yup." Another pre-pubescent male (MV-5), approximately seven to eight years old based on body stature and lack of pubic hair, who is wearing a black shirt with lettering which reads, "Any game any time", is standing near MV-3 and his erect penis is visible. MV-4 stands and MV-3 continues to perform oral sex on MV-4. A voice can be heard saying, "…..do it at the same time." Another voice can be heard saying, "you have to move up and down." MV-3 then begins to perform oral sex MV-5 and the camera is moved positioned near MV-5's penis. This continues for approximately twenty-six seconds. MV-3 then performs oral sex on MV-4. MV-5 is visible fondling his penis. MV-3 briefly continues to perform oral sex on MV-4 but returns to performing oral sex on MV-5. MV-5 momentarily removes his penis from the mouth of MV-3 and begins to masturbate. A voice can be heard saying, "Are you going to cum?" MV-3 is observed fondling the penis of MV-5 and again continues to perform oral sex as MV-5 begins to thrust his thighs. MV-3 stops performing oral sex and uses right hand to remove ejaculate from his upper lip as a voice is heard indicating, "Good job." MV-3 continues to perform oral sex on MV-5 and briefly stops and indicates, "You're so wet." The camera then focuses on MV-5 as he begins to masturbate with his right hand. MV-3 then continues to perform oral sex and the video concludes.*

Based on my training and experience, the video as described above depicts child pornography.

25. In addition to the above records and information, Google provided the preserved video described in paragraph thirteen which produced the NCMEC CyberTip.

26. On May 23, 2023, a subpoena was issued to Google LLC requesting records to be produced for email account mikejacobs989fg@gmail.com.

27. On May 24, 2023, Google provided records indicating this account was created on November 26, 2021. The name listed for this account is Mike Jacobs. IP login records were provided from December 1, 2022 to May 18, 2023.

SEARCH WARRANT EXECUTED AT THE RESIDENCE OF MICHAEL D. JACOBS AND CONSENSUAL INTERVIEW CONDUCTED

28. On June 6, 2023, the U.S. District Court for the Eastern District of Wisconsin (case no. 23-m-378) authorized a search warrant for Michael D. JACOBS JR.'s residence located at 1711 South 68th Street, West Allis, Wisconsin.

29. On June 14, 2023, at approximately 0604 hours, special agents, and detectives with HSI Milwaukee and the West Allis Police Department executed a search warrant at 1711 South 68th Street, West Allis, Wisconsin. Encountered during the execution of this search warrant were Michael D. JACOBS JR. and his father Michael D. Jacobs Sr.

30. During a subsequent interview conducted with Michael Jacobs Sr., he stated a cellular telephone located in the residence belonged to him, but his son always used it. He believed this device could be located in his son's room. He also stated a laptop computer located in the residence belonged to his son and was located in his son's room. Jacobs Sr. denied viewing child sexual abuse material (CSAM).

31. Additionally, on this date, Michael D. JACOBS JR. was interviewed at the West Allis Police Department. Prior to conducting this interview, JACOBS JR. was

advised of his rights to counsel which he voluntarily waived in writing. JACOBS JR. admitted to registering and using the email address of burningtempest1989@gmail.com. He indicated no other individual had access to this account. He stated, "I should have probably relayed this to the registry" and "…a video I came across and I'm ashamed of it. I viewed it and I tried sharing it….I think it was boys or something like that." He admitted to downloading the video using the Tor browser on his father's cell phone.

32. JACOBS JR. also recalled saving one video to the Google Drive account associated with burningtempest1989@gmail.com. He admitted to emailing a Google Drive link containing the video which he recalled depicted a "a boy on a man" performing oral sex. He also recalled the man performing oral sex on two, minor males. When asked if he recalled the video depicting two minors standing behind and penetrating the adult male, JACOBS JR. stated, "something like that……sounds familiar." He described this video as being child pornography based on the age of the minors.

33. When questioned about a second video send on January 19, 2023 from email address burningtempest1989@gmail.com to mikejacobs989fg@gmail.com, JACOBS JR. did recall sending this video which described as being, "boys I think." After the video description was read to him, JACOBS JR. indicated he was familiar with this video and after viewing it he thought to himself, "what I am doing looking at this?" He affirmed this video depicted CSAM. He stated he initially saved the video to the "documents" folder. He indicated, "I think I may have deleted it."

34. JACOBS JR. admitted to accessing the Tor browser "every few weeks or something like that." He also admitted, "there probably will be a few more other videos" which he obtained from the Tor browser and downloaded to the "documents" folder. He indicated he deleted these files after a "few weeks." He clarified he downloaded approximately seven to eight videos which all depicted CSAM. JACOBS JR. stated he has fantasized about having sexual intercourse with minors and last did "a few days ago."

35. JACOBS JR. was not arrested and allowed to return to his residence. He relocated to a new residence located at 822 W. Scott Street, #6, Milwaukee, Wisconsin on June 29, 2023 based on information received from his U.S. Probation Officer.

FORENSIC EXAMINATIONS COMPLETED ON ELECTRONIC DEVICES

36. Seized during the execution of the search warrant at 1711 South 68th Street, West Allis, Wisconsin were multiple electronic devices including a Western Digital 320 GB hard drive removed from a Dell desktop computer and a Google Pixel cellular telephone.

37. I have reviewed items recovered from the Western Digital 320 GB hard drive. Recovered from this device were approximately 216 files which depict CSAM. Approximately 131 of these files are in a video format. A video file labeled as "fla85F.tmp" is described as follows:

> *This video is fifty-four seconds in length and begins by the camera focusing on the vagina of a female toddler, approximately three to four years of age based on body stature. An adult male is observed placing the tip of his penis into the vagina of the toddler. The toddler is then observed repositioning herself on her knees and elbows exposing her*

buttock. The adult male begins to insert his penis into the buttock area of the toddler and the video concludes.

38. An image file labeled as 3T3nRNrlY-sKs3R0MH-0rmTFep8yKNqtdfr—Q4mGYw[1].jpg also recovered from this device is described as follows:

This is an image which depicts a minor female approximately eight to ten years of age based on body stature. She is wearing a green shirt and is kneeling. The minor female's arms are pressed against the thigh area of a naked adult male. The unclothed lower torso and upper thigh area are visible in the image. The minor female has handcuffs around her wrists and is observed performing oral sex.

39. Recovered from the residence was also a Google Pixel 6a cellular telephone. This device was located in the bedroom of JACOBS JR. Items recovered from this device include approximately four video files which depict CSAM. A video files labeled as .trashed-1687122825-3yo Masy aka Beauty (HQ-60fps-x265).mp4 is described as follows:

This video is approximately fifteen minutes in length and begins with an adult male who is seated. The adult male is wearing a white shirt and no pants. He can be seen holding his penis with his right hand. His upper torso area is not visible. A female toddler with long blonde hair, who is approximately two to three years of age based upon her body stature, is visible in the image and is not wearing a shirt. As the video begins, the adult male is holding a sign which reads, "This one's for you, Bum Yum!!!" The adult male lifts the child up and places her on his lap between his slightly spread legs. The child is wearing a diaper which the adult male removes exposing her vagina. The adult male repositions her so she is in an inclined position and begins to fondle her bare vagina with this right index finger. The video continues with the adult male performing various sexual acts on this child including putting his erect penis inside her mouth and also putting his erect penis inside her anus. The child can be heard on the video saying, "dadda."

INDICTMENT, ARREST, AND INTERVIEW OF MICHAEL D. JACOBS JR.

40. On November 7, 2023, Michael D. JACOBS JR. was indicted by a grand jury sitting in the Eastern District of Wisconsin for one count of Possession of Child Pornography (case no. 23-CR-201) in violation of 18 U.S.C. 2252A(a)(5)(B) and

2252A(b)(2). On this date, the U.S. District Court for the Eastern District of Wisconsin issued an arrest warrant for JACOBS JR.

41. On November 8, 2023, HSI special agents, deputies with the U.S. Marshal's Service, and an investigator with the West Allis Police Department executed an arrest warrant at the residence of JACOBS JR. located at 822 W. Scott Street, #6, Milwaukee, Wisconsin. Prior to departing the residence, JACOBS JR. indicated he wished to bring his cellular telephone, later determined to be a Samsung Galaxy S9, Model SM-G960U1. After being advised of his rights to having counsel present during questioning and informing him an arrest warrant had been issued, JACOBS JR. agreed to speak to law enforcement.

42. During a subsequent interview conducted with JACOBS JR., he acknowledged any CSAM located on a Google Pixel cellular telephone previously located in his room would have been files he had downloaded and viewed. He also acknowledged last using a desktop computer (containing the Western Digital 320 GB hard drive) approximately eight years ago which was also recovered from his residence during the execution of the search warrant. When questioned about downloading and viewing CSAM files located on this device, JACOBS JR. indicated, "I probably did, but I just don't remember doing it because it's been such a long time ago."

43. During the interview, JACOBS JR. consented to a search of his Samsung Galaxy cellular telephone by law enforcement. JACOBS JR. admitted to downloading and viewing CSAM files on this device approximately five weeks ago while using the Tor browser. He estimated he viewed "four or five" files and then deleted them.

44. JACOBS JR. also admitted a tablet electronic device, later determined to be a BLU tablet, Model M8L 2022, could be located in his current room which he, "got it through a government program…a month or two ago." JACOBS JR. admitted to viewing CSAM on this device "four or five weeks ago" while using the Tor browser. He indicated no other individual has accessed this device. JACOBS JR. indicated he used an open internet connect at his current residence to download the CSAM files. JACOBS JR. provided verbal consent to law enforcement allowing a search of his room, as well as the tablet located in it.

SEARCH WARRANTS EXECUTED ON SEIZED ELECTRONIC DEVICES AND INFORMATION OBTAINED FROM NCMEC

45. On November 16, 2023, a search warrant was authorized by the U.S. District Court for the Eastern District of Wisconsin (23-mj-204) to search the Samsung Galaxy S9, Model SM-G960U1 and BLU tablet, Model M8L 2022 seized of JACOBS JR's apartment. Forensic examinations conducted on these devices resulted in the recovery of no CSAM files. Recovered from the BLU tablet, Model M8L 2022 were user accounts associated with email addresses mikejacobsjr1989af@gmail.com and soramaro989xz@gmail.com.

46. On November 20, 2023, email addresses mikejacobsjr1989af@gmail.com and soramaro989xz@gmail.com were provided to NCMEC to inquire if any CyberTipline reports were associated with these accounts. On this date, NCMEC indicated CyberTipline report 175785267 was submitted by Dropbox, Inc and associated with "mikejacobsjr*".

47. On November 20, 2023, I received CyberTip report #175785267 from NCMEC indicating a Dropbox account associated with a verified email address of mikejacobsjr1989af@gmail.com was reportedly used to possession, manufacture, and distribute child pornography. This account was registered on October 6, 2023, at 05:03:50 UTC, from IP address 2603:6000:a600:6b1:d21d:2cdf:b799:4182. A login occurred on October 6, 2023, at 05:06:30 UTC, from IP address 2603:6000:a600:6b1:104:31c9:af37:e0b. Dropbox provided a file labeled as ks12yo(dvdr).divx.mkv which was viewed by Dropbox personnel and categorized as a pubescent minor engaged in sexual intercourse.

48. On November 29, 2023, a subpoena was issued to Google requesting records associated with email address mikejacobsjr1989af@gmail.com. Records received indicate this account was created on September 20, 2023. The name listed for this account is "Mike Jacobs." The last login into this account occurred on November 8, 2023, at 12:17:23 UTC, from IP address 2603:6000:a600:6b1:298f:abf4:607f:5147.

49. On November 29, 2023, a subpoena was issued to Dropbox, Inc. requesting records and information for a Dropbox account associated with mikejacobsjr1989af@gmail.com. Records received indicate this account was created on October 6, 2023 at 05:03:50 UTC. An authentication log provided indicates on October 6, 2023, at 05:03:50 UTC, this account was authenticated from IP address 2603:6000:a600:6b1:d21d:2cdf:b799:4182. The name provided for this account is "mike jacobs."

50. On December 4, 2023, a subpoena was issued to Charter Communications, Inc. requesting records and information for IP addresses associated with the aforementioned NCMEC CyberTip report, Google account, and Dropbox account. Records subsequently received indicate these IP addresses were assigned to Recovery Network, 822 W. Scott St., Milwaukee, Wisconsin. This address, as previously noted, was the apartment building where JACOBS JR. resided since June 29, 2023 until the time of his arrest on November 8, 2023.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

51. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox to disclose to the government copies of the records and other information (including the content of communications).

52. Based on the forgoing, I request that the Court issue the proposed search warrant.

53. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

55. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Dropbox who will then compile the

requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

The property to be searched is the entire digital contents of the Dropbox account(s) associated with the email account mikejacobsjr1989af@gmail.com and all its associated services including deleted files and e-mails; IP addresses and associated dates/times used to access the e-mail account; that is/are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 1800 Owens Street, San Francisco, California 94158.

ATTACHMENT B

I. Information to be disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. 2703(f), Dropbox is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox account described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting: and emails "invites" sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during

registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. 2252 involving accounts associated with the Dropbox links files referenced in Attachment A, including information pertaining to the following matters:

a. Possession, receipt, and distribution of child pornography images and/or videos;

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation;

c. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user of the Dropbox accounts about matters relating to the possession, receipt, and distribution of child pornography, including records that help reveal their whereabouts.

III. Method of Delivery

Items seized pursuant to this search warrant can be served by sending it on any digital media device, via FedEx or U.S. Mail, to Special Agent Nathan Cravatta, 790 N. Milwaukee Street, Suite 600, Milwaukee, Wisconsin, 53202, via email to Nathan.A.Cravatta@hsi.dhs.gov, or provided via Dropbox's Law Enforcement and Government Online Submission System.